Cybersecurity Incident Report: Network Traffic Analysis

The UDP protocol reveals that: The UDP (User Datagram Protocol) was used to send the DNS query from the browser to the DNS server. This protocol is associated with the request to resolve the domain name `www.yummyrecipesforme.com` into an IP address.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: The ICMP error message received was “udp port 53 unreachable.” This indicates that the UDP packet sent to port 53 of the DNS server could not be delivered.

The port noted in the error message is used for: Port 53 is used for DNS (Domain Name System) services. It is the standard port for both DNS queries and responses over UDP.

The most likely issue is: The most likely issue is that the DNS server at IP address `203.0.113.2` was not reachable on port 53, meaning the server was either down or not listening on the DNS port, resulting in the “udp port 53 unreachable” error.

Incident Analysis

Time Incident Occurred: The incident occurred at 13:24:32.192571 (1:24 p.m.). This timestamp is based on the log entries captured by the network analyzer tool, `tcpdump`, which recorded the events leading up to and including the error message.

Explain How the IT Team Became Aware of the Incident: The IT team became aware of the incident through client reports indicating they were unable to access the website `www.yummyrecipesforme.com`. Clients experienced the error message “destination port unreachable” when trying to load the page. This issue was then replicated and observed by the IT team, prompting further investigation using network analysis tools.

Explain the Actions Taken by the IT Department to Investigate the Incident:

1. **Initial Diagnosis:** The IT team attempted to visit the affected website themselves and encountered the same issue, confirming that the problem was not isolated to clients.
2. **Network Analysis:** The team used the `tcpdump` tool to capture network traffic and analyze the packets. This involved sending a DNS query to a DNS server and examining the responses.
3. **Error Analysis:** The captured data showed ICMP error messages indicating that UDP packets could not reach port 53 on the DNS server. This helped identify the nature and source of the problem.

Note Key Findings of the IT Department's Investigation:

Port Affected: Port 53, which is used for DNS services, was reported as unreachable.

- **DNS Server Impacted:** The DNS server with IP address `203.0.113.2` was the target of the UDP packets.
- **Error Message:** The ICMP error message “udp port 53 unreachable” was received, indicating that the DNS server was not available or not listening on port 53.

Note a Likely Cause of the Incident: The likely cause of the incident is that the DNS server at IP address `203.0.113.2` was either down or not functioning properly on port 53, leading to the “udp port 53

unreachable" error. This prevented the DNS queries from being processed and resolved, causing the reported access issues to the website.

Summary of the Problem Found in the `tcpdump` Log

Brief Summary:

The `tcpdump` log analysis revealed that DNS queries sent from your computer to the DNS server encountered an issue. The log captured UDP traffic for DNS queries and ICMP error messages indicating problems with the DNS service. Specifically:

- **DNS Query:** The log showed UDP packets being sent from your computer to the DNS server at IP address `203.0.113.2` on port 53, which is used for DNS services. These packets were intended to resolve the domain name `www.yummyrecipesforme.com` to an IP address.
- **ICMP Error Response:** The log also included ICMP error messages with the text "udp port 53 unreachable." This indicates that the UDP packets sent to the DNS server's port 53 could not be delivered, meaning the server was not reachable or not accepting requests on that port.

Protocols Used:

- **UDP (User Datagram Protocol):** Used for sending DNS queries from your computer to the DNS server. UDP is the protocol that handles DNS requests and responses.
- **ICMP (Internet Control Message Protocol):** Used for sending error messages back to your computer, indicating that the UDP packets could not reach port 53 on the DNS server.

In summary, the `tcpdump` log analysis identified that DNS queries using UDP were not successful due to ICMP errors indicating that port 53 on the DNS server was unreachable.

Part One: Cybersecurity Incident Report

Summary of `tcpdump` Log Analysis:

After analyzing the data from the `tcpdump` log, the following trends and details were identified:

- **Protocols Used:**
  - UDP (User Datagram Protocol): Used for sending DNS queries from your computer to the DNS server.
  - ICMP (Internet Control Message Protocol): Used for sending error messages from the DNS server back to your computer.
- **Details Indicated in the Log:**

    - The log showed that UDP packets were sent to port 53 on the DNS server at IP address `203.0.113.2`.
    - ICMP error messages were returned with the text “udp port 53 unreachable,” indicating that the UDP packets could not be delivered to port 53 on the DNS server.
- **Interpretation of Issues Found:**
    - Protocol Generating the Error: The error message was generated in response to UDP traffic. The ICMP error messages indicated that UDP traffic to port 53 was not reaching the DNS server.
    - Port 53: This port is commonly used for DNS services. The repeated mention of port 53 in the error messages suggests that the DNS server was either down or not accepting traffic on this port.

In summary, the `tcpdump` log analysis revealed that UDP queries to port 53 were unsuccessful due to ICMP error messages indicating that the port was unreachable. This suggests an issue with the DNS server's availability or configuration on port 53, impacting DNS resolution for `www.yummyrecipesforme.com`

Part Two: Cybersecurity Incident Report

When the Problem Was First Reported: The problem was first reported on [specific date], when several clients encountered issues accessing the website `www.yummyrecipesforme.com`. They received the error message “destination port unreachable” while trying to load the page.

Scenario, Events, and Symptoms Identified When the Event Was First Reported:

- **Scenario:** Clients reported being unable to access the website `www.yummyrecipesforme.com`.
- **Events:** Users experienced a “destination port unreachable” error message after attempting to access the site.
- **Symptoms:** The symptom was the inability to reach the website, leading to failed DNS queries and a subsequent inability to resolve the domain name to its corresponding IP address.

Current Status of the Issue: The issue is currently under investigation. The initial findings indicate that the DNS server’s port 53 is unreachable, affecting the ability to resolve DNS queries for the website.

Information Discovered While Investigating the Issue Up to This Point:

- **Traffic Log Analysis:** The `tcpdump` log revealed UDP traffic being sent to port 53 of the DNS server and ICMP error messages stating “udp port 53 unreachable.”
- **Protocols Involved:** The UDP protocol was used for the DNS queries, and ICMP was used for reporting the errors.
- **Port Affected:** Port 53, which is crucial for DNS services, was identified as being unreachable.

Next Steps in Troubleshooting and Resolving the Issue:

1. **Verify DNS Server Status:** Check the status of the DNS server at IP address `203.0.113.2` to confirm if it is operational and correctly configured.
2. **Examine Network Connectivity:** Investigate network connectivity issues that may be affecting the ability to reach port 53 on the DNS server.
3. **Review Firewall and Security Settings:** Check firewall and security settings that might be blocking UDP traffic on port 53.
4. **Test DNS Server Availability:** Perform further tests to ensure the DNS server is actively listening on port 53 and able to process incoming queries.

Suspected Root Cause of the Problem: The suspected root cause of the problem is that the DNS server at IP address `203.0.113.2` is either down or not listening on port 53. This unavailability of port 53, which is critical for DNS services, has resulted in the ICMP error messages and the inability to resolve DNS queries for **`www.yummyrecipesforme.com`**.